9920 v21.2.2.0 Deployment Guide

Installation, Configuration, and Network Packet Broker Management

9039083-00 Rev AA
October 2024

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

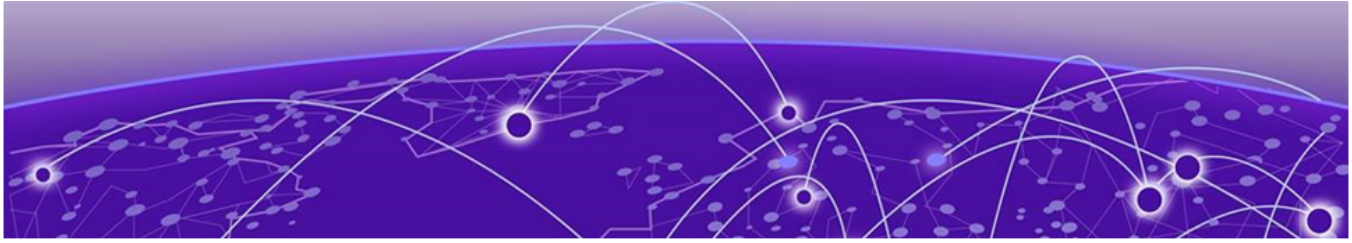
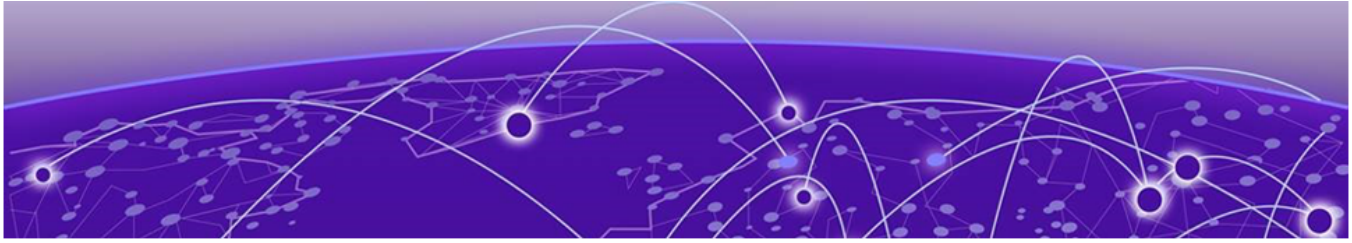


Table of Contents



Abstract

The 9920 Deployment Guide for software version 21.2.2.0 provides in-depth instructions for deploying the 9920 platform as a network packet broker (NPB). It details installation and upgrade processes using multiple protocols, including USB, NFS, HTTP, FTP, and TFTP. Core functionalities include support for link aggregation, traffic replication, load balancing, and advanced ACL filtering for high-performance traffic management. Additional features include packet slicing, tunnel origination and termination for both IPv4 and IPv6, and encapsulation stripping to optimize visibility applications. The guide also addresses the firmware upgrade process, covering microservice updates for critical subsystems such as packet handling and security. The deployment process relies heavily on CLI for precise configuration, management, and troubleshooting in complex network environments.

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

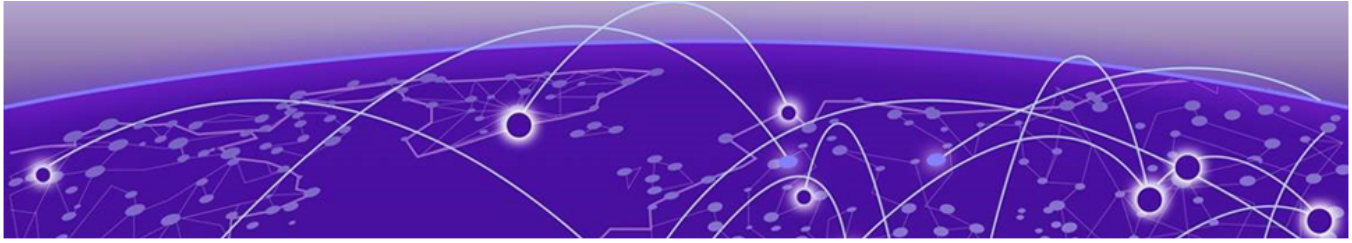
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

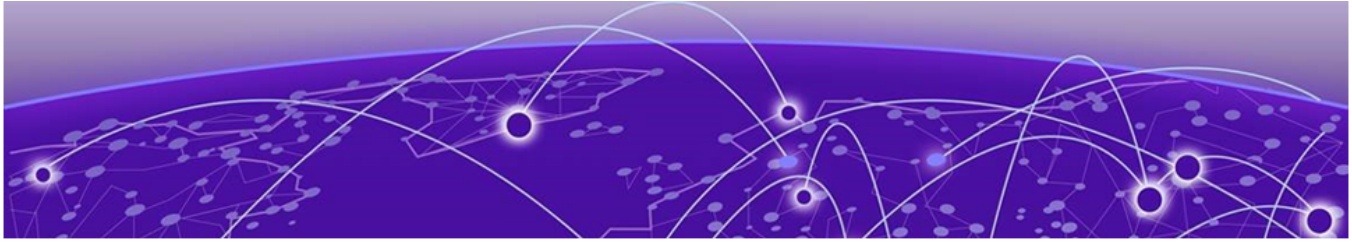
Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



What's New in this Document

There are no changes to this guide for the Extreme 9920 software, release 21.2.2.0.

For more information about this release, see the *Extreme 9920 Software Release Notes, 21.2.2.0*.



Deployment Preparation

The NPB software runs the NPB operating system and provides network packet broker functions.

NPB Application Overview

The NPB application provides network packet broker functions to process and prepare packets for visibility tools. This allows core networking devices to offload network monitoring.

When the Extreme 9920 device running Extreme 9920 software is attached to optical taps between the core networking devices, a copy of the traffic is sent to the Extreme 9920 device for filtering the traffic of interest, formatting it, and sending it on to visibility tools.

The NPB application supports the following network packet broker functions:

- Link Aggregation: Aggregates traffic arriving from multiple ports and directs it to a single port or port-channel ("many to one").

  Link Aggregation Control Protocol (LACP): Enables devices to send Link Aggregation Control Protocol Data Units (LACPDUs) to each other and establish link aggregation connections.
- Replication: Replicates network traffic to multiple ports and port-channels ("one to many").
- Load balancing: Distributes network traffic among ports in a port-channel.
- ACL filtering: Directs network traffic based on Layer 2 to Layer 4 protocol headers.
- Route-map forwarding: Redirects packets based on Layer 2 to Layer 4 Protocol headers to the desired physical port or port-channel interfaces.
- Packet slicing: Truncates the packet to a specified length.
- Tunnel origination or encapsulation: Encapsulates packets with IPv4 Generic Routing Encapsulation (GRE) headers.
- Tunnel termination: Classifies and decapsulates incoming IPv4 and IPv6 packets.
- Encapsulation-header stripping:
  - Removes tags that are not supported by visibility applications.

    - Supports 802.1BR, VN-Tag, VLAN, VXLAN, GTPU, GRE, and IPIP headers.
- Quality of Service (QoS): Provides preferential treatment to specific traffic that is received on multiple ingress interfaces or Test Access Points (TAPs).
- Link Layer Discovery Protocol (LLDP): Allows network devices to advertise their identity and capabilities to peer devices on a LAN and store information about the network.

Supported Device Information

The Extreme 9920 software with the NPB application runs on Extreme 9920 devices.

Extreme 9920 Software

Extreme 9920 software consists of OS software and microservices that provide various services and functionality.

The build script builds images for all modules and forms a ONIE compatible bin image during installation for both net-install and firmware update.

The Extreme 9920 software image, `TierraOS-<release_no>-NPB.bin`, is a binary file and contains all components except ONIE (bootloader). Extreme 9920 software images can be downloaded from http://engartifacts1.extremenetworks.com:8089/artifactory/tierra-local-snapshots/build/.

You can download the Extreme 9920 software image from a remote server using any of the following methods:

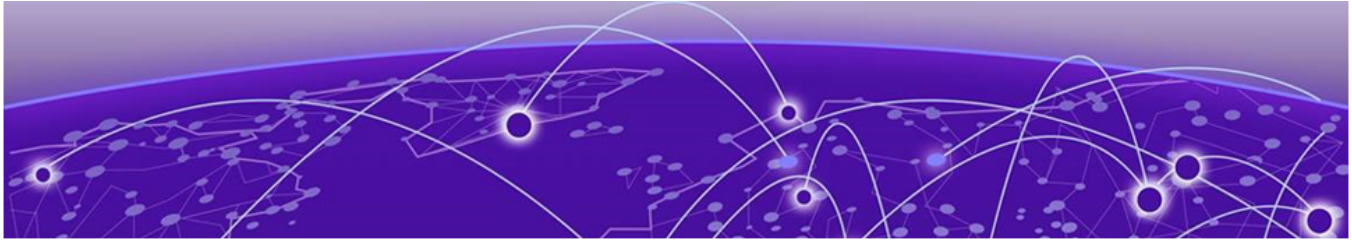
- Prepared USB 3.0 device
- Remote NFS share
- HTTP
- FTP
- TFTP

Extreme 9920 Software Operating System

Extreme 9920 software Operating System (TierraOS) is built using the standard ONLPv2 procedure. Installation of Extreme 9920 software is done using Open Networking Install Environment (ONIE) standard.

ONIE is the combination of a boot loader and a small operating system for bare metal network devices that provides an environment for automated provisioning or recovery of the device. The Extreme 9920 device boots the software from the images stored on the hard disk of the device. ONIE also provides mechanisms to re-install or update the software if the normal software download process fails.

The process supported by the **`system firmware upgrade`** command is not affected by this feature. The Extreme 9920 software is not updated to the snapshot partition during the normal upgrade process.



Installation and Upgrade

The topics in this section provide the information required to install and upgrade the Extreme 9920 software.

Install Extreme 9920 Software

Before You Begin

- Throughout the installation process, a serial console must be connected to the device.
- The out-of-band management Ethernet interface must be connected if you are using a remote NFS share, HTTP, FTP, or TFTP:
  - Availability of a DHCP server on the LAN for this Ethernet interface might enable you to skip the need to manually configure the ONIE to connect to one of the network-based methods of transferring the software.
  - If a DHCP server is not available, you need the default gateway, network mask, and an IP address that is not in use on the network to which the Ethernet interface is connected.

About This Task

You can download the Extreme 9920 software image from a remote server using any of the following methods:

- Prepared USB 3.0 device
- Remote NFS share
- HTTP
- FTP
- TFTP

Perform the following steps from the serial console.

Procedure

1. Access the ONIE Recovery Shell.
   a. Reboot the device using the CLI or power-cycle.
   b. When the BIOS splash screen is displayed, use the **Down Arrow** key to access the GRUB boot menu and stop the boot timer.
   c. Select **ONIE** from the first menu, and press the **Down Arrow** key to stop the boot timer.
   d. Select **ONIE: Rescue**, and press **Enter** when prompted.

      The ONIE shell opens.

   You can use ONIE for recovering or upgrading the device.
2. Perform one of the following:
   - If a DHCP server is running on the network, proceed to the next step.
   - If you are using a remote server to download the firmware, go to step 5 on page 13.
3. Check connectivity to the server hosting the software.
   a. Ping the remote server from which you intend to download the software.
   b. If the ping fails, run the following commands to gather information on the connection state.

      ```
      ip addr
      ip route show
      ifconfig
      ```

      If there are any errors, perform step 4 to resolve them. Otherwise, proceed to step 5 on page 13.
4. Configure static networking on eth0 for ONIE.
   a. Add the IP address to the eth0 interface.

      ```
      ONIE:/ #ip addr add <ip-addr/mask> dev eth0
      ```

   b. Configure the default gateway.

      ```
      ONIE:/ #ip route add default via <gateway-ip-addr> dev eth0
      ```
5. Download and install the Extreme 9920 software firmware using one of the following remote server methods:
   - Perform USB Disk-Based Recovery on page 14
   - Perform NFS-Based Recovery on page 14
   - Perform HTTP-Based Recovery on page 15
   - Perform FTP-Based Recovery on page 15
   - Perform TFTP-Based Recovery on page 16

   A checksum validation is done before installing the firmware.
6. Activate the firmware using `Activate gRPCs`.
7. Verify if the installation is successful using `Verify gRPCs`.

Perform USB Disk-Based Recovery

Procedure

1. From the serial console, download and decompress the software tarball.
2. Transfer the resulting directory to an inserted USB 3.0 device.
3. Eject or unmount the USB device and insert it into the USB port on the front panel of the Extreme 9920 device.
4. Run the **`fdisk -l`** command. In the output, locate the device identifier of the inserted USB device.

   The USB device is generally the last device listed.
5. Run the **`mkdir /media`** and **`mount /dev/<device-identifier> /media`** commands.

   You might see a warning, but the disk should mount.
6. Change directory to the Network Packet Broker software that you want to install and start the installation using the `onie-nos-installer file: //`.
7. Select the binary file for the Extreme 9920.

   ```
   ONIE:/ #cd media/
   ONIE:/ media/ #ls ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
   ```

   The device reboots and loads the software.

Perform NFS-Based Recovery

Procedure

1. On a Linux device, configure an NFS share, download and decompress the software tarball, and move the resulting directory to the root of the NFS share.
2. On the Extreme 9920 device, configure and verify network connectivity to the server.
   a. Configure the network.

      ```
      # ifconfig eth1 10.139.69.108 netmask 255.255.254.0 up
      ```

   b. Configure the default route.

      ```
      # route add default gw 10.139.69.1
      ```

   c. Verify network connectivity to the server.

      ```
      # ping 10.139.69.1
      ```
3. Run the **`mkdir /media`** and **`mount :/<path-to-NFS-share>/ /media`** commands.

   If an error results, troubleshoot the **`mount`** command. You might need more parameters or a more explicit path.
4. Change directory to the Network Packet Broker software that you want to install and start the installation using the `onie-nos-installer file: //`.
5. Select the binary file for the Extreme 9920.

   ```
   ONIE:/ #cd media/

   ONIE:/ media/ #ls ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
   ```

   The process takes approximately 15 to 20 minutes to complete. The device reboots and loads the software.

Perform HTTP-Based Recovery

Procedure

1. On a web server, download and decompress the software tarball and move the resulting directory to the root of the web server.
2. Modify the permissions of the directory to allow access for the web server daemon.
3. Verify that the software directory is accessible by using a web browser to access the directory.
4. On the Extreme 9920, configure and verify network connectivity to the server.
   a. Configure the network.
      ```
      # ifconfig eth1 10.139.69.108 netmask 255.255.254.0 up
      ```
   b. Configure the default route.
      ```
      # route add default gw 10.139.69.1
      ```
   c. Verify network connectivity to the server.
      ```
      # ping 10.139.69.1
      ```
5. Run the **onie-nos-install** command with the URL to the binary for the device.
   ```
   ONIE:/ #onie-nos-install http://<URL-to-binary>/
   ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
   ```

Perform FTP-Based Recovery

Procedure

1. On an FTP server, download and decompress the software tarball and move the resulting directory to the root of the FTP server.
2. Modify the permissions of the directory to allow access for the FTP server daemon. The FTP server must allow anonymous access.
3. Verify that the software directory is accessible by using an FTP client to access the directory.
4. On the Extreme 9920 device, configure and verify network connectivity to the server.
   a. Configure the network.
      ```
      # ifconfig eth1 10.139.69.108 netmask 255.255.254.0 up
      ```
   b. Configure the default route.
      ```
      # route add default gw 10.139.69.1
      ```
   c. Verify network connectivity to the server.
      ```
      # ping 10.139.69.1
      ```
5. Run the **onie-nos-install** command with the URL to the binary for the device.
   ```
   ONIE:/ #onie-nos-install http://<URL-to-binary>/
   ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
   ```

Perform TFTP-Based Recovery

Procedure

1. On a TFTP server, download and decompress the software tarball and move the resulting directory to the root of the TFTP server.
2. Modify the permissions of the directory to allow access for the TFTP server daemon.
3. On the Extreme 9920 device, configure and verify network connectivity to the server.
   a. Configure the network.
      ```
      # ifconfig eth1 10.139.69.108 netmask 255.255.254.0 up
      ```
   b. Configure the default route.
      ```
      # route add default gw 10.139.69.1
      ```
   c. Verify network connectivity to the server.
      ```
      # ping 10.139.69.1
      ```

   TFTP might appear to be non-operational while transferring the file.
4. Run the **onie-nos-install** command with the URL to the binary for the device.
   ```
   ONIE:/ #onie-nos-install http://<URL-to-binary>/
   ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
   ```

View Firmware Version Information

Procedure

1. View the primary and secondary firmware version information.
   ```
   show firmware
   ```
2. View the last five firmware versions activated on the device.
   ```
   show firmware history
   ```
3. View the firmware logging information.
   ```
   show logging audit firmware
   ```

Upgrade the Extreme 9920 Firmware

The Extreme 9920 firmware contains primary and secondary images. When new firmware is installed, the image in the secondary location is removed and the image in the primary location is moved to the secondary location. The new image is installed in the primary location.

About This Task

Take the following steps to upgrade the firmware.

Procedure

1. Back up the running configuration on the device.

   You will restore the backed up configuration after you upgrade the firmware.
   ```
   # copy running-config flash://config-file/<yourconfig.cfg>
   ```

2. Copy the default configuration on the device.

```
# copy default-config running-config
```

3. Upgrade the firmware using one of the following commands.

```
# system firmware update flash://firmware/filename

# system firmware update usb://filename

# system firmware update scp://username:password@host[:port]/filepath

# system firmware update sftp://username:password@host[:port]/filepath

# system firmware update http://[username:password@]host[:port]/filepath

# system firmware update https://[username:password@]host[:port]/filepath
```

Both IPv4 and IPv6 addresses are supported.

- If the firmware update is successful, the system is rebooted automatically to activate the new version.

  The reboot reason is updated to `RR_UPGRADE` to indicate firmware update or rollback. The reboot reason is stored in the `chassis-0` property.

- Configurations persist after reboot, and all microservices are expected to come up. When the microservices come up, the `Firmware Rev` property in the `chassis-0` component is published to `State DB` with the running firmware image.
- If any microservice fails to come up within the specified duration, an automatic rollback to the previous image is triggered.

4. Restore the backed up configuration.

```
# copy flash://config-file/<yourconfig.cfg> running-config
```

5. (Optional) If the new firmware version is not required, revert to the previous version.

```
# system firmware rollback
```

Supported Microservice Upgrades

Extreme 9920 software supports the following microservice upgrades:

- chassis-mgr
- interface-agent
- interface-mgr
- lacp
- nexthop-agent
- packet-mgr
- pbd-agent
- pcap-agent
- pipeline-agent
- security
- sfcs-agent

- snmp
- svcplane-agent
- target-proxy-agent

Upgrade Microservices

About This Task

Microservice images are `tar.gz` files. Each `tar.gz` file contains a `manifest.json` file with the service name and version number.

Before You Begin

- Microservice upgrade must be performed in the maintenance window.
- Ensure that there is no change in the configuration during the upgrade procedure.

Procedure

1. Copy the microservice image to the device using SCP, SFTP, HTTP, or HTTPS.
2. Update the required microservice using the appropriate command.

```
# system service update flash://ms-images/filename

# system service update usb://filename

# system service update scp://username:password@host[:port]/filepath

# system service update sftp://username:password@host[:port]/filepath

# system service update http://[username:password@]host[:port]/filepath

# system service update https://[username:password@]host[:port]/filepath
```

   Both IPv4 and IPv6 addresses are supported.
3. Activate the new version.
   - All previous microservice images are saved at `flash://ms-images/<service-name> directories`.

     There is no limit to the number of files saved on the disk other than disk space. However, the files are removed if the firmware is upgraded.
   - The current service stops and the new service starts.
   - Service shutdown handler is invoked as part of the **`kubectl set image`** command.
   - The microservice handles graceful shutdown or recovery and sets the restart reason (`MSSR_UPGRADE`). When the new version of the microservice comes up, it checks the restart reason and takes necessary steps to be operational again.
4. (Optional) If the new microservice version is not required, roll back to the previous running version.

```
# system service rollback service-name
```

5. (Optional) Activate any of the previous versions of the microservice.

```
# system service update flash://ms-images/<service-name> directories
```

After rollback, if any of the services do not come up, the `Status` property for `chassis-0` component is set to `Degraded` state.